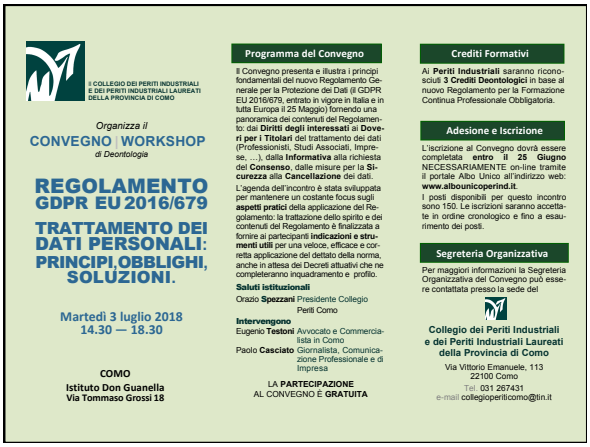


IL COLLEGIO DEI PERITI INDUSTRIALI E DEI PERITI INDUSTRIALI LAUREATI DELLA PROVINCIA DI COMO

Organizza il

CONVEGNO | WORKSHOP

di Deontologia

REGOLAMENTO GDPR EU 2016/679

TRATTAMENTO DEI DATI PERSONALI: PRINCIPI, OBBLIGHI, SOLUZIONI.

Martedì 3 luglio 2018
14.30 — 18.30

COMO
Istituto Don Guanella
Via Tommaso Grossi 18

Programma del Convegno

Il Convegno presenta e illustra i principi fondamentali del nuovo Regolamento Generale per la Protezione dei Dati (il GDPR EU 2016/679, entrato in vigore in Italia e in tutta Europa il 25 Maggio) fornendo una panoramica dei contenuti del Regolamento: dai **Diritti degli interessati** ai **Doveri per i Titolari** del trattamento dei dati (Professionisti, Studi Associati, Imprese, ...), dalla **Informativa** alla richiesta del **Consenso**, dalle misure per la **Sicurezza** alla **Cancellazione** dei dati.

L'agenda dell'incontro è stata sviluppata per mantenere un costante focus sugli **aspetti pratici** della applicazione del Regolamento: la trattazione dello spirito e dei contenuti del Regolamento è finalizzata a fornire ai partecipanti **indicazioni e strumenti utili** per una veloce, efficace e corretta applicazione del dettato della norma, anche in attesa dei Decreti attuativi che ne completeranno inquadramento e profilo.

Saluti istituzionali

Orazio **Spezzani** Presidente Collegio Periti Como

Intervengono

Eugenio **Testoni** Avvocato e Commercialista in Como

Paolo **Casciato** Giornalista, Comunicazione Professionale e di Impresa

LA **PARTECIPAZIONE** AL CONVEGNO È **GRATUITA**

Crediti Formativi

Ai **Periti Industriali** saranno riconosciuti **3 Crediti Deontologici** in base al nuovo Regolamento per la Formazione Continua Professionale Obbligatoria.

Adesione e Iscrizione

L'iscrizione al Convegno dovrà essere completata **entro il 25 Giugno** NECESSARIAMENTE on-line tramite il portale Albo Unico all'indirizzo web: **www.albounicoperind.it**.

I posti disponibili per questo incontro sono 150. Le iscrizioni saranno accettate in ordine cronologico e fino a esaurimento dei posti.

Segreteria Organizzativa

Per maggiori informazioni la Segreteria Organizzativa del Convegno può essere contattata presso la sede del

Collegio dei Periti Industriali e dei Periti Industriali Laureati della Provincia di Como
Via Vittorio Emanuele, 113
22100 Como
Tel. 031 267431
e-mail collegioperiticomo@tin.it

Programma

- **Introduzione** al **Regolamento Generale sulla Protezione dei Dati** (GDPR) **EU 2016/679**
- **Principi Ispiratori** e **Fondamenti**
- **Definizioni** e **Ruoli**
- **Attività** e **Strumenti**

A tutela dei diritti fondamentali e delle libertà dei cittadini, il **Garante per la Protezione dei dati personali** ha poteri di carattere regolamentare, di vigilanza e inibitori.

www.garanteprivacy.it

BEN OLTRE LA PRIVACY…

Il diritto alla privacy cambia dalla tradizionale **immunità della sfera privata** dagli sguardi altrui **a strumento di difesa della persona** dall'ingerenza del potere, privato e pubblico, e dalle molteplici forme di controllo in cui esso si esercita.

IL GDPR METTE AL CENTRO DELLA TUTELA LE PERSONE E I LORO DIRITTI

I NOSTRI DIRITTI

- Essere **informati** in modo trasparente, leale e dinamico se, da chi e il modo in cui nostri dati personali vengono **raccolti, trattati, profilati, archiviati**
- **Sapere quali dati vengono trattati**
- **Controllare**, **correggere** e **opporsi**
- Diritto alla **portabilità** dei dati
- Diritto a **cancellazione e oblio**
- Diritto di essere informati su eventuali **violazioni** dei propri dati personali
- Diritto di proporre **reclamo** all'Autorità

La tutela dei dati personali è importante perché…

I **dati personali** sono un **bene economico** e **svolgono una funzione sociale**

Identificare una persona in modo diretto o indiretto (social…) significa **poterla o volerla trattare in modo diverso rispetto a un'altra.**

La situazione in Italia

- Nonostante la diretta applicabilità e vincolatività del GDPR, l'art. 13 della L. 25.10.2017 n. 163 aveva delegato il Governo ad adottare uno o più decreti legislativi, **entro il 21 maggio 2018**, al fine di adeguare il quadro normativo nazionale al GDPR. Sono gli "Attuativi" che stiamo aspettando…

La situazione in Italia

- *Bye bye Dlgs 196 del 30.06.2003*
- Il Codice *in vigore dal 01.01.2004* dal 25.05. 2018 **non vale più.**
- I Decreti attuativi arriveranno e inizieranno le verifiche sulla conformità al GDPR: by design e by default: Non ci facciamo trovare impreparati!

Con l'obiettivo di promuovere un profondo positivo **cambiamento culturale** nel modo in cui oggi i dati personali vengono trattati (e concessi) sia on-line sia off-line…

…il GDPR punta sulla **responsabilizzazione** di chi raccoglie, tratta o fa trattare dati personali…

…oltre su una più matura diffusa **consapevolezza** dell'importanza di proteggere **identità e reputazione** reali e virtuali: ciò che viene definito come autodeterminazione informativa.

Il **Titolare del trattamento** è tenuto a porre in essere misure tecniche e organizzative per garantire **ed essere in grado di dimostrare** che il trattamento dei dati è effettuato nel rispetto del GDPR.

Il **Titolare del trattamento** in caso di ispezione non risponderà alla domanda ***"ha fatto...?"*** bensì alla più complessa e onerosa domanda aperta: ***"Cosa ha fatto per...?"***

Non solo soldi…

- L'adeguamento al GDPR non richiede — nella maggioranza dei casi — un investimento economico rilevante ma un approccio differente, organizzativo e strategico alla materia.

RUOLI E DEFINIZIONI

(principali...)

Trattamento dei dati personali

- Qualsiasi operazione compiuta con o senza processi automatizzati relativa a dati o insiemi di dati personali:
  - Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, trasmissione o diffusione, raffronto o interconnessione, limitazione, cancellazione o distruzione, …

Principi applicabili al trattamento dei dati personali

- I principi di base del trattamento dei dati personali secondo il GDPR includono:
  - Liceità e Finalità
  - Correttezza e Trasparenza
  - Minimizzazione
  - Limitazione della conservazione

Dati personali: cosa sono?

- Qualsiasi informazione riguardante **persone fisiche (NON giuridiche)** identificate o identificabili ("interessati") direttamente o indirettamente, con particolare riferimento a nome e cognome, dati relativi all'ubicazione, identificativi online…
- **Identificativi**, **sensibili**, **giudiziari**

Dati personali: cosa sono?

- Qualsiasi informazione riguardante **persone fisiche (NON giuridiche)** con particolare riferimento a uno o più elementi caratteristici della loro **identità fisica**, **fisiologica**, **genetica**, **psichica**, **economica**, **culturale** o **sociale**, **reati** e **condanne penali**, …

Applicabilità materiale e territoriale

- Il Regolamento si applica:
  - Ai trattamenti effettuati nel territorio dell'Unione Europea (a prescindere se i dati si trovino o no in EU);
  - Ai trattamenti relativi a persone, servizi, proposte, attività, comportamenti che avvengano in Europa;
  - **Approccio garantista: nel dubbio si applica il GDPR**

Titolare del Trattamento

- Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

Contitolari del Trattamento

- Due o più Titolari che determinano congiuntamente, mediante accordo interno e in modo trasparente le rispettive responsabilità, finalità e mezzi del trattamento, in particolare riguardo i diritti degli interessati.

Responsabile del Trattamento

- Effettua il trattamento dei dati per conto del Titolare
- Presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate per garantire la tutela dei diritti dell'interessato.

Responsabile del Trattamento

- Opera in base a un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che lo vincoli e specifichi tutti gli aspetti della materia affidata.

Incaricato del Trattamento

- Dipendenti, Professionisti, Tirocinanti e tutte le persone chiamate a gestire dati personali. Devono essere esplicitamente autorizzati, meglio se per iscritto.

Incaricato del Trattamento

- Dipendenti, Professionisti, Tirocinanti e tutte le persone chiamate a gestire dati personali devono essere informate, sensibilizzate e formate sui principi del GDPR e sulle modalità operative adottate, inclusa la gestione di documenti e password.

Rappresentante del Titolare del Trattamento stabilito all'estero

- Persona fisica o giuridica stabilita nell'Unione Europea che, designata per iscritto dal Titolare del trattamento o dal Responsabile del trattamento, li rappresenta per quanto riguarda gli obblighi dettati dal GDPR.

Responsabile della Protezione dei Dati (*Data Protection Officer*)

- Persona fisica o giuridica, Autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- Indipendenza, Autorevolezza e competenza manageriale;
- Tra i suoi compiti la sensibilizzazione e formazione del personale.

Responsabile della Protezione dei Dati (*Data Protection Officer*)

- Obbligatorio nel caso di:
  - Autorità / Organismi pubblici
  - **Monitoraggio regolare e sistematico di dati personali su larga scala**
  - Trattamento, su larga scala, di **categorie particolari di dati personali** (Artt. 9 e 10)

Trattamento

- Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o a insiemi di dati personali.

Trattamento | 2 **Ad esempio:**

- Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione di dati personali.

Profilazione

- Qualsiasi forma di trattamento automatizzato di dati personali consistente nel loro utilizzo per valutare aspetti personali relativi a una persona fisica…

Profilazione

…in particolare per analizzarne o prevederne aspetti riguardanti rendimento professionale, situazione economica, salute, preferenze personali, interessi, affidabilità, comportamento, ubicazione o spostamenti.

Archivio

- Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, a prescindere dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito su base geografica o funzionale, cartaceo o elettronico.

Liceità e Finalità del trattamento

- Ai fini della sua **liceità**, ogni trattamento deve trovare fondamento in un'*idonea base giuridica* che, oltre al Consenso, è determinata dalle seguenti condizioni:
  a) Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

Liceità e Finalità del trattamento

Il trattamento è necessario:

b) Per adempiere un obbligo legale al quale è soggetto il titolare del medesimo;
c) Per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
d) Per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

Liceità e Finalità del trattamento

Il trattamento è necessario:

e) Per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Dati adeguati, pertinenti e limitati

I dati personali trattati devono essere:

- **Adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per cui sono trattati ("minimizzazione dei dati");
- **Esatti e aggiornati**;
- **Tempestivamente cancellati** oppure **rettificati** se inesatti e rispetto alle finalità.

Integrità e riservatezza dei dati

- I dati devono essere trattati in maniera da **garantire un'adeguata sicurezza** — compresa la protezione mediante misure tecniche e organizzative — da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione o dal danno accidentali.

Modulo Informativa e Richiesta Consenso

- Va predisposto uno **specifico modulo di informativa** sulle specifiche attività di trattamento dei dati personali, sulle finalità, la durata, l'eventuale comunicazione a terzi e/o trasferimento all'estero, etc., **e per la raccolta del consenso.**

Modulo Informativa e Richiesta Consenso

- Il modulo deve includere specifici riferimenti alle attività svolte da ciascun Titolare del trattamento, dunque **non è possibile prevedere un modulo** standard, "uguale per tutti", e che sia valido per tutti.
- Ciascuno deve sviluppare il proprio Modulo per Info e Consenso!

Consenso

- È una qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso mediante dichiarazione o azione positiva inequivocabile al fatto che i propri dati personali siano oggetto di trattamento (e a quale tipo).

Consenso

- Per la raccolta del consenso sono ammessi mezzi elettronici — quali la selezione di un'apposita casella in un sito web — o orali *(principio di libertà delle forme)*;
- ***Non dovrebbero*** **configurare consenso il silenzio, l'inattività o la preselezione di caselle**

Consenso

- In base al principio della responsabilizzazione, il Titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato inequivocabilmente il proprio consenso al trattamento dei propri dati personali.

Revoca del consenso

- L'interessato ha il diritto di revocare il consenso in qualsiasi momento
- La revoca non pregiudica la liceità del trattamento effettuato in base al consenso precedentemente dato
- Il diritto di revoca deve essere indicato nell'informativa per l'espressione del consenso.

Revoca del consenso

- **Il consenso deve poter essere revocato con la stessa facilità con cui è stato accordato:** vanno previste le medesime forme e/o misure tecniche utilizzate al momento della raccolta del consenso.

Protezione e sicurezza dei dati

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio e che comprendono, tra le altre, se del caso:

Protezione e sicurezza dei dati

a. La pseudonimizzazione e la cifratura dei dati personali;
b. La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c. La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d. Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Valutazione di Impatto (DPIA)

- *(Art. 35)* Quando un tipo di trattamento — allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento — può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Valutazione di Impatto (DPIA)

- La valutazione d'impatto sulla è richiesta in particolare nei casi seguenti:
  a) Valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni con effetti giuridici che incidono in modo analogo significativamente su dette persone fisiche;
  b) Il trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; *oppure*
  c) La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Valutazione di Impatto (DPIA)

- Per chi è tenuto *(di sicuro: Ospedali, Autostrade, Aziende nei confronti di dipendenti, …)* è disponibile anche in Italiano un software, sviluppato dalla Autorità Garante Francese:

PIA

https://www.cnil.fr/en/privacy-impact-assessment-pia

Rischi

- I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico materiale o immateriale
- La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

Violazione dei dati personali (*Data Breach*)

- **Premessa**: Vanno poste in essere misure per la prevenzione di violazioni di sicurezza che comportino accidentalmente o in modo illecito distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o comunque trattati.

Violazione dei dati personali (*Data Breach*)

- Eventuali violazioni, le relative circostanze e conseguenze, e i provvedimenti adottati vanno **documentati** per agevolare l'adozione delle misure necessarie e per dimostrare al Garante, su richiesta in caso di accertamenti, quanto accaduto, deciso e attuato.

Notifica in caso di violazioni

- I Titolari del trattamento devono notificare al Garante eventuali violazioni di dati personali **senza ingiustificato ritardo** e entro 72 ore dalla scoperta soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Notifica in caso di violazioni

- I Titolari del trattamento devono informare gli interessati, senza ingiustificato ritardo **soltanto** se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati
- Qualora ciò richiedesse sforzi sproporzionati, è ammessa una comunicazione pubblica di pari efficacia

Registro delle Attività

- Obbligatorio per imprese e organizzazioni con oltre 250 dipendenti se vengono trattati dati sensibili, genetici, biometrici, giudiziari; se il trattamento non è occasionale e se possa presentare un rischio per i diritti e le libertà degli interessati.

Registro delle Attività

- Non obbligatorio ma raccomandabile in tutti gli altri casi per guidare lo sviluppo e la realizzazione del proprio modello organizzativo e di sicurezza, e per dimostrare il proprio impegno di analisi in caso di verifiche esterne.

Sanzioni

- "Le Autorità di controllo provvedono affinché le sanzioni amministrative pecuniarie inflitte in relazione a violazioni del Regolamento siano in ogni singolo caso **effettive, proporzionate e dissuasive**.".

Sanzioni

- La violazione delle disposizioni relative agli obblighi del Titolare del trattamento e del Responsabile del trattamento è soggetta a sanzioni amministrative pecuniarie **fino a 10 milioni** di Euro **o** per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Sanzioni

- Le sanzioni salgono fino a **20 milioni** di Euro, o per le imprese **fino al 4%** del fatturato mondiale totale annuo dell'esercizio precedente se superiore in caso di violazioni a:
  - Principi di base del trattamento, incluso il consenso;
  - Diritti degli interessati;
  - Trasferimenti di dati personali a destinatari in Paesi terzi o organizzazioni internazionali.

Consulenti ed esperti…

- Attualmente non sono previsti specifici requisiti professionali e/o obblighi formativi per i soggetti che intendano fornire consulenza in materia di privacy o assumere l'incarico di Responsabile della Protezione dei Dati.
- Attendiamo l'emanazione dei Decreti delegati, e che il Garante elabori eventuali ulteriori indicazioni.

GDPR EU 2016/679
General Data Protection Regulation

Cosa c'è da sapere e cosa fare

Responsabilizzazione e Autovalutazione del rischio

- In virtù del principio di responsabilizzazione dei Titolari del trattamento dei dati, il GDPR non definisce modelli, attività o strumenti "**obbligatori**" ma indica gli obiettivi da raggiungere mediante una autovalutazione del rischio e l'individuazione di modalità di gestione appropriate dei dati: "by design" e "by default".

Come "**autovalutarsi**"?

- Da soli, una volta compresi spirito, obiettivi e dettato del GDPR
- Utilizzando un software dedicato. A pagamento?
- Utilizzando PIA
- …

Cosa **autovalutare** (in **15 punti**)

Quali informazioni raccogliere?

1. Chi è e come contattare il Titolare / i Contitolari del trattamento
2. Chi è il Responsabile del trattamento
3. Chi è [se c'è] il Responsabile della Protezione dei Dati (DPO)
4. Chi è / Chi sono gli Incaricati del trattamento? Sono stati formati e "sensibilizzati"? Come? Quando?

Quali informazioni raccogliere?

5. Quali dati raccogliamo, di chi, perché; su quale base giuridica (incarico, mandato, obbligo, consenso, …)
6. Come acquisiamo i dati?
7. Come trattiamo i dati (archivi cartacei, informatici, software, profilazione). Sistemi automatizzati?

Quali informazioni raccogliere?

8. Come e dove trattiamo e archiviamo i dati? (se all'estero anche il Paese)
9. Comunichiamo o condividiamo i dati? A chi/Con chi? Perché? Come?
10. Come / Quando aggiorniamo e prevediamo di cancellare i dati?
11. Quali sono rischi e misure di protezione e sicurezza in relazione al trattamento dei dati?

Quali informazioni raccogliere?

12. Come gestiamo eventuali richieste degli Interessati?
13. Procedura in caso di violazioni?
14. Quali sono i diritti degli interessati Come li informiamo dei loro diritti?
15. Modulo **Informativa e richiesta del Consenso** da consegnare, illustrare e far firmare dagli interessati

Cosa vogliamo preparare?

- Schema di Modulo per Informativa e Consenso
- Schema di Registro delle Attività
- Lettera di Incarico
- …

Su Carta Intestata del Professionista / Studio

Modulo Informativa e Consenso

Informativa ai sensi dell'Art. 13 del Regolamento Europeo 679/2016 (GDPR) e richiesta del Suo consenso

Ai sensi dell'Art. 13 del Regolamento Europeo 2016/679 e in relazione ai Suoi dati personali Le comunichiamo quanto segue:

1. …
2. …
3. …
4. …

Cosa avevamo detto?

- Essere **informati** in modo trasparente, leale e dinamico se, da chi e il modo in cui nostri dati personali vengono **raccolti, trattati, profilati, archiviati**
- **Sapere quali dati vengono trattati**
- **Controllare**, **correggere** e **opporsi**
- Diritto alla **portabilità** dei dati
- Diritto a **cancellazione e oblio**
- Diritto di essere informati su eventuali **violazioni** dei propri dati personali
- Diritto di proporre **reclamo** all'Autorità

Modello fac-simile da adattare ai casi specifici

CARTA INTESTATA PROFESSIONISTA | STUDIO

Informativa ai sensi dell'Art. 13 del Regolamento Europeo 679/2016 (GDPR) e richiesta del Suo consenso

Ai sensi dell'Art. 13 del Regolamento Europeo 2016/679 e in relazione ai Suoi dati personali Le comunic____ quanto segue:

Titolare del trattamento dei dati personali

Titolare del trattamento dei dati personali è nella persona di (qui indicato anche come "professionista") con domicilio eletto presso lo Studio situato in . Il Titolare del trattamento dei dati può essere contattato all'indirizzo e-mail:

Tipologia di dati

Minimizziamo sia la tipologia dei Suoi dati raccolti sia la durata dell'archiviazione. I dati personali da noi trattati sono raccolti direttamente da Lei e includono informazioni necessarie per la Sua identificazione, tra cui il Suo domicilio e Suoi dati di contatto, così come – se necessario per lo svolgimento dell'incarico da Lei affidatoci – categorie particolari di dati, in conformità con l'Articolo 9 del GDPR.

Finalità e Modalità del trattamento dei dati

Il trattamento è finalizzato alla corretta e completa esecuzione dell'incarico professionale da Lei ricevuto, all'adempimento degli obblighi previsti in ambito fiscale e contabile, al rispetto degli obblighi incombenti sul professionista e prevalsi dalla normativa vigente, nonché all'invio di nostre Circolari e Comunicazioni relative ad argomenti inerenti i servizi a Lei forniti. I Suoi dati possono essere trattati a mezzo di archivi cartacei, elettronici e telematici, con logiche strettamente correlate alle modalità appropriate per far fronte alle finalità sopra indicate.

Base giuridica del trattamento

Lo Studio tratta i Suoi dati personali in modo lecito e corretto. Il trattamento deve essere necessario per lo svolgimento di un Suo mandato, di un contratto di cui Lei è parte, per l'esecuzione di misure precontrattuali adottate su Sua richiesta o per adempiere obblighi di legge incombenti sul professionista.

Natura obbligatoria o facoltativa del conferimento e conseguenze della mancata comunicazione dei dati personali

Con riguardo ai dati personali relativi all'esecuzione del contratto di cui Lei è parte o relativi all'adempimento a un obbligo normativo (ad esempio per la tenuta di scritture contabili e fiscali), la mancata comunicazione dei dati personali impedisce il perfezionarsi del rapporto contrattuale stesso.

Conservazione dei dati

I Suoi dati personali saranno conservati per le finalità sopra indicate, saranno conservati per il periodo di durata del contratto e, successivamente, per il tempo in cui il professionista sia soggetto a obblighi di conservazione per finalità fiscali o altre previsti, da norme di legge o regolamenti.

Comunicazione dei dati

I Suoi dati personali potranno essere comunicati a:

1. Commercialisti, Avvocati o altri professionisti che eroghino prestazioni funzionali ai fini sopra indicati;
2. Istituti bancari e assicurativi che eroghino prestazioni funzionali ai fini sopra indicati;
3. Soggetti che elaborano i dati in esecuzione di specifici obblighi di legge;
4. Autorità giudiziarie o amministrative, per l'adempimento degli obblighi di legge.

Profilazione e Diffusione

I Suoi dati personali non sono soggetti a diffusione a terzi estranei né ad alcun processo decisionale interamente automatizzato, ivi comprese la profilazione.

Diritti dell'Interessato

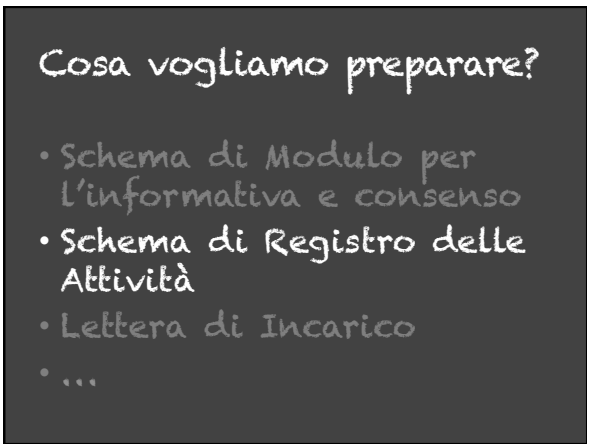
Tra i diritti a Lei riconosciuti dal GDPR rientrano quelli di:

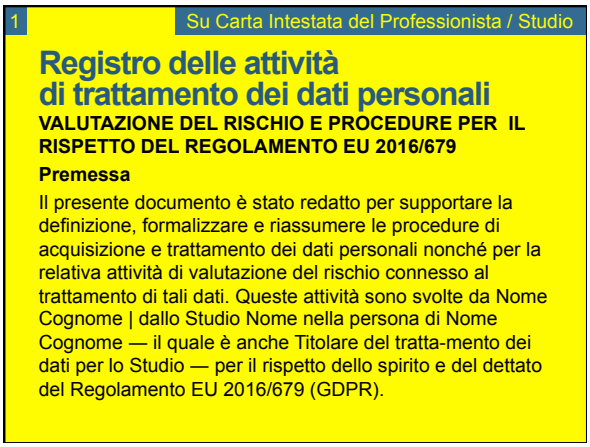
- Chiedere al professionista l'accesso ai Suoi dati personali e alle informazioni relative agli stessi; la rettifica dei dati inesatti o l'integrazione di quelli incompleti; la cancellazione dei dati personali che La riguardano (al verificarsi di una delle condizioni indicate nell'art. 17, par.1 del GDPR e nel rispetto delle eccezioni previste nel par. 3 dello stesso articolo); la limitazione del trattamento dei Suoi dati personali (al ricorrere di una delle ipotesi indicate nell'art. 18, par.1 del GDPR);
- Richiedere e ottenere dal professionista – nelle ipotesi in cui la base giuridica del trattamento sia il contratto o il consenso, e lo stesso sia effettuato con mezzi automatizzati – i Suoi dati personali in formato strutturato e leggibile da dispositivo automatico, anche perché Lei possa comunicare tali dati a un altro Titolare del trattamento (diritto alla portabilità dei dati personali);
- Opporsi in qualsiasi momento al trattamento dei Suoi dati personali al ricorrere di situazioni particolari che La riguardano;
- Revocare il consenso in qualsiasi momento limitatamente a cui il trattamento sia basato sul Suo consenso per una o più specifiche finalità e riguardi dati personali comuni (ad esempio data e luogo di nascita o luogo di residenza), oppure particolari categorie di dati (ad esempio dati che rivelano la Sua opinioni politiche, convinzioni religiose, il Suo stato di salute). Il trattamento basato sul consenso ed effettuato antecedentemente alla revoca conserva comunque la sua liceità;
- Essere informato in caso di violazioni dei Suoi dati;
- Proporre reclamo a una Autorità di controllo quale l'Autorità Garante per la protezione dei dati personali, il cui sito internet è www.garanteprivacy.it.

Io sottoscritt_____ Codice Fiscale _____ acconsento che il professionista ponga in essere le attività sopra descritte per le quali il mio consenso rappresenti la base giuridica del trattamento, e:

☐ Presto il consenso *oppure* ☐ Nego il consenso

Luogo e data, _____ Firma leggibile dell'Interessato _____





Registro delle attività di trattamento dei dati personali

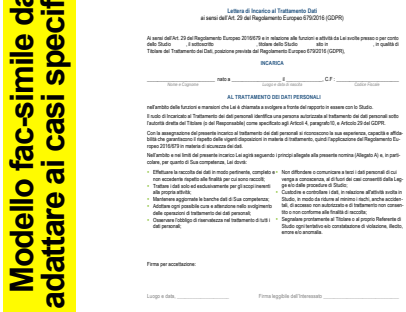
CONTENUTI INDICATIVI

- Premessa
- Titolare del trattamento
- Tipologia di dati trattati
- Modalità di acquisizione dei dati
- Modalità di trattamento e archiviazione
- Comunicazione, Diffusione e Profilazione dei Dati
- Luogo del trattamento
- Personale incaricato del trattamento
- Modalità del trattamento dei dati:
  - Schedari cartacei e altri supporti informatici
  - Elaboratori dotati di connessione internet
- Postazioni PC e Server
- Fax
- Archiviazione documenti e fascicoli elettronici e cartacei
- Protezioni e Sicurezza
- Formazione e sensibilizzazione del personale incaricato del trattamento
- **Analisi dei Rischi**

Cosa vogliamo preparare?

- Schema di Modulo per l'informativa e consenso
- Schema di Registro delle Attività
- Lettera di Incarico
- ...

Modello fac-simile da adattare ai casi specifici



Lettera di Incarico al Trattamento Dati
ai sensi dell'Art. 29 del Regolamento Europeo 679/2016 (GDPR)

Ai sensi dell'Art. 29 del Regolamento Europeo 2016/679 e in relazione alle funzioni e attività da Lei svolte presso o per conto dello Studio il sottoscritto titolare dello Studio sito in in qualità di Titolare del Trattamento dei Dati, posizione prevista dal Regolamento Europeo 679/2016 (GDPR),

INCARICA

_____ nato a _____ il _____ C.F.: _____
Nome e Cognome — Luogo e data di nascita — Codice Fiscale

AL TRATTAMENTO DEI DATI PERSONALI

nell'ambito delle funzioni e mansioni che Lei è chiamata a svolgere a fronte del rapporto in essere con lo Studio.

Il ruolo di Incaricato al Trattamento dei dati personali identifica una persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare (o del Responsabile) come specificato agli Articoli 4, paragrafo10, e Articolo 29 del GDPR.

Con la assegnazione del presente incarico al trattamento dei dati personali si riconoscono la sua esperienza, capacità e affidabilità che garantiscono il rispetto delle vigenti disposizioni in materia di trattamento, quindi l'applicazione del Regolamento Europeo 2016/679 in materia di sicurezza dei dati.

Nell'ambito e nei limiti del presente incarico Lei agirà seguendo i principi allegati alla presente nomina (Allegato A) e, in particolare, per quanto di Sua competenza, Lei dovrà:

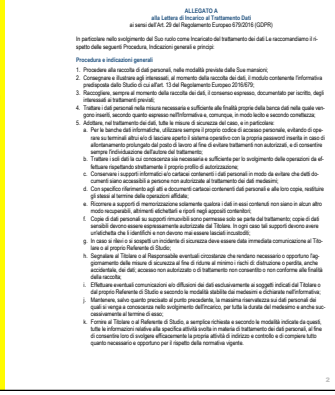
- Effettuare la raccolta dei dati in modo pertinente, completo e non eccedente rispetto alle finalità per cui sono raccolti;
- Trattare i dati solo ed esclusivamente per gli scopi inerenti alla propria attività;
- Mantenere aggiornate le banche dati di Sua competenza;
- Adottare ogni possibile cura e attenzione nello svolgimento delle operazioni di trattamento dei dati personali;
- Osservare l'obbligo di riservatezza nel trattamento di tutti i dati personali;
- Non diffondere o comunicare a terzi i dati personali di cui venga a conoscenza, al di fuori dei casi consentiti dalla Legge e/o dalle procedure di Studio;
- Custodire e controllare i dati, in relazione all'attività svolta in Studio, in modo da ridurre al minimo i rischi, anche accidentali, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità di raccolta;
- Segnalare prontamente al Titolare o al proprio Referente di Studio ogni tentativo e/o constatazione di violazione, illecito, errore e/o anomalia.

Firma per accettazione:

Luogo e data _____ Firma leggibile dell'Interessato _____

Allegati: Allegato A

Modello fac-simile da adattare ai casi specifici



ALLEGATO A
alla Lettera di Incarico al Trattamento Dati
ai sensi dell'Art. 29 del Regolamento Europeo 679/2016 (GDPR)

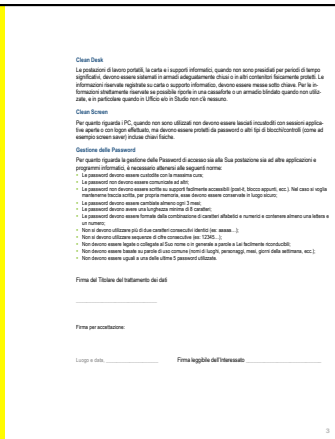
In particolare nello svolgimento del Suo ruolo come Incaricato del trattamento dei dati Le raccomandiamo il rispetto delle seguenti Procedure, Indicazioni generali e principi:

Procedure e indicazioni generali

1. Procedere alla raccolta di dati personali, nelle modalità previste dalle Sue mansioni;
2. Consegnare e illustrare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa predisposta dallo Studio di cui all'art. 13 del Regolamento Europeo 2016/679;
3. Raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti;
4. Trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;
5. Adottare, nel trattamento dei dati, tutte le misure di sicurezza del caso, e in particolare:
   a. Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento prolungato dal posto di lavoro al fine di evitare trattamenti non autorizzati, e di consentire sempre l'individuazione dell'autore del trattamento;
   b. Trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
   c. Conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
   d. Con specifico riferimento agli atti e documenti cartacei contenenti dati personali e alle loro copie, restituire gli stessi al termine delle operazioni affidate;
   e. Riporre e supporti di memorizzazione solamente qualora i dati in essi contenuti non siano in alcun altro modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
   f. Copie di dati personali su supporti rimuovibili sono permesse solo se parte del trattamento; copie di dati sensibili devono essere espressamente autorizzate dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
   g. In caso si rilevi o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare o al proprio Referente di Studio;
   h. Segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario o opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;
   i. Effettuare eventuali comunicazioni e/o diffusioni dei dati esclusivamente ai soggetti indicati dal Titolare o dal proprio Referente di Studio e secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
   j. Mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo e anche successivamente al termine di esso;
   k. Fornire al Titolare o al Referente di Studio, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative alla specifica attività svolta in materia di trattamento dei dati personali, al fine di consentire loro di svolgere efficacemente la propria attività di indirizzo e controllo e di compiere tutto quanto necessario e opportuno per il rispetto della normativa vigente.

2

Modello fac-simile da adattare ai casi specifici



Clean Desk

Le postazioni di lavoro portatili, le carte e i supporti informatici, quando non sono presidiati per periodi di tempo significativi, devono essere sistemati in armadi adeguatamente chiusi o in altri contenitori fisicamente protetti. Le informazioni riservate registrate su carta o supporto informatico, devono essere messe sotto chiave. Per le informazioni strettamente riservate se possibile riporle in una cassaforte o un armadio blindato quando non utilizzate, e in particolare quando in Ufficio e/o in Studio non c'è nessuno.

Clean Screen

Per quanto riguarda i PC, quando non sono utilizzati non devono essere lasciati incustoditi con sessioni applicative aperte o con logon effettuato, ma devono essere protetti da password o altri tipi di blocchi/controlli (come ad esempio screen saver) inclusi chiavi fisiche.

Gestione delle Password

Per quanto riguarda la gestione delle Password di accesso sia alla Sua postazione sia ad altre applicazioni e programmi informatici, è necessario attenersi alle seguenti norme:

- Le password devono essere custodite con la massima cura;
- Le password non devono essere comunicate ad altri;
- Le password non devono essere scritte su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, esse devono essere conservate in luogo sicuro;
- Le password devono essere cambiate almeno ogni 3 mesi;
- Le password devono avere una lunghezza minima di 8 caratteri;
- Le password devono essere formate dalla combinazione di caratteri alfabetici e numerici e contenere almeno una lettera e un numero;
- Non si devono utilizzare più di due caratteri consecutivi identici (ex: aaaaa...);
- Non si devono utilizzare sequenze di cifre consecutive (ex: 12345...);
- Non devono essere legate o collegate al Suo nome o in generale a parole a Lei facilmente riconducibili;
- Non devono essere basate su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.);
- Non devono essere uguali a una delle ultime 5 password utilizzate.

Firma del Titolare del trattamento dei dati

_____

Firma per accettazione:

Luogo e data _____ Firma leggibile dell'Interessato _____

3

Monitoraggio e aggiornamento

- **Le procedure adottate dovranno essere costantemente monitorate e aggiornate in base sia all'evoluzione delle norme regolamentari sia ad eventuali modifiche di vostri assetti organizzativi interni.**